Algebraic geometric construction of a quantum stabilizer code

Ryutaroh Matsumoto
Department of Communications and Integrated Systems
Tokyo Institute of Technology, 152-8552 Japan
Email: ryutaroh@rmatsumoto.org

August 8, 2001

Abstract

The stabilizer code is the most general algebraic construction of quantum error-correcting codes proposed so far. A stabilizer code can be constructed from a self-orthogonal subspace of a symplectic space over a finite field. We propose a construction method of such a self-orthogonal space using an algebraic curve. By using the proposed method we construct an asymptotically good sequence of binary stabilizer codes. As a byproduct we improve the Ashikhmin-Litsyn-Tsfasman bound of quantum codes. The main results in this paper can be understood without knowledge of quantum mechanics.

1 Introduction

Recently quantum computation and quantum communication have attracted much attention, because the use of quantum mechanical phenomena can offer unusual efficiency in computation and communication. We have to protect quantum states from environmental noise in quantum computation and some methods in quantum communication, such as the quantum superdense coding [3, 4]. The quantum error-correcting codes (or quantum codes) independently proposed by Shor [18] and Steane [19] is one of techniques for protecting quantum states. Recently it was recognized that construction of quantum codes is connected with the problem of finding a linear space over a finite field with certain properties (see Theorem 1). In this paper we propose a method of constructing such linear spaces from an algebraic curve.

Let us explain quantum codes and their connection with linear spaces over finite fields. We begin with the notion of t-error correction. Let $\mathcal{H}$ be a q-dimensional complex linear space, where q is a prime power, and suppose that $\mathcal{H}$ represents a physical system of interest. A quantum code Q is a q^k-dimensional subspace of $\mathcal{H}^{\otimes n}$. When we want to protect a quantum state in $|\varphi\rangle \in \mathcal{H}^{\otimes k}$, we encode $|\varphi\rangle$ into a state in Q. So we encode a quantum state of k particles into that of n particles. Suppose that we send $|\varphi\rangle \in Q$ and receive $|\psi\rangle \in \mathcal{H}^{\otimes n}$. A quantum code Q is said to be *t-error-correcting* if we can decode $|\varphi\rangle$ from $|\psi\rangle$ provided that at least the states of $n-t$ particles in $|\psi\rangle$ are left unchanged from $|\varphi\rangle$.

Since a change of a quantum state is continuous, the notion of t-error correction seems nonsense at first glance [12]. This notion can be justified as follows: In general the decoding process of a quantum code does not decode perfectly the transmitted quantum state from a received one. However, the decoded state and a transmitted state become closer as t increases provided that the quantum channel used is memoryless as a q-ary channel [16, Section 7.4], [14]. A quantitative relation between the closeness of states, the noisiness of a channel, and t can be found in [14].

In [14] it is shown that one can make the decoded state arbitrary close to the transmitted state by increasing the code length provided that the ratio t/n is fixed and is sufficiently large compared with the noisiness of the channel. This is a major motivation for studying long codes as in the classical coding theory [15, Section 4.3]. When the code length is small, we can find good quantum codes by examining all possible codes by a computer. However, when the code length is large, we need some systematic construction method for producing good quantum codes. In this paper we propose such a method.

We are now able to state the connection between quantum codes and finite fields, which is obtained for the binary code ($\dim \mathcal{H} = 2$) by Calderbank et al. [5, 6] and generalized to the nonbinary case by Ashikhmin and Knill [1]. Let $\mathbf{F}_q$ be the finite field with q elements. For vectors $\vec{x} = (x_1, \ldots, x_{2n})$ and $\vec{y} = (y_1, \ldots, y_{2n}) \in \mathbf{F}_q^{2n}$ we define the standard symplectic form (or alternating form) by

$$\langle \vec{x}, \vec{y} \rangle_{\mathrm{s}} = \sum_{i=1}^{n} x_i y_{n+i} - \sum_{i=1}^{n} x_{n+i} y_i. \tag{1}$$

A linear space with a nondegenerate symplectic form is called a symplectic space. For a vector $\vec{x} \in \mathbf{F}_q^{2n}$ define the weight of $\vec{x}$ by

$$w(\vec{x}) = \sharp\{1 \le i \le n \mid (x_i, x_{n+i}) \ne (0,0)\}. \tag{2}$$

For a subspace $C \subset \mathbf{F}_q^{2n}$ we define

$$C^{\perp \mathrm{s}} = \{\vec{x} \in \mathbf{F}_q^{2n} \mid \forall \vec{y} \in C,\ \langle \vec{x}, \vec{y} \rangle_{\mathrm{s}} = 0\},$$

that is, the orthogonal space of C with respect to (1).

Theorem 1 *[1, 5, 6] If there is an $(n+k)$-dimensional subspace $C \subset \mathbf{F}_q^{2n}$ such that $C \supseteq C^{\perp \mathrm{s}}$, then we can construct a $\lfloor (d(C \setminus C^{\perp \mathrm{s}}) - 1)/2 \rfloor$-error-correcting quantum code $Q \subset \mathcal{H}^{\otimes n}$ of dimension q^k, where*

$$d(C \setminus C^{\perp \mathrm{s}}) = \min\{w(\vec{x}) \mid \vec{x} \in C \setminus C^{\perp \mathrm{s}}\}.$$

The quantum code Q constructed by this method is called a *stabilizer code* and is proposed independently by Gottesman [11] and Calderbank et al. [5, 6]. The nonbinary generalization is due to Knill [13] and Rains [17]. The stabilizer code is the most general algebraic construction of quantum codes proposed so far.

The value $d(C \setminus C^{\perp \mathrm{s}})$ is called the *minimum distance* of a stabilizer code. A stabilizer code with minimum distance d encoding k particles into n particles is called an $[[n, k, d]]$ code.

Rains [17, p.1831, Remarks] observed that a $q_1 q_2$-ary stabilizer code is a tensor product of a q_1-ary stabilizer code and a q_2-ary one if q_1 and q_2 are relatively prime. So we restrict ourselves to stabilizer codes for quantum systems of prime power dimension.

This paper is organized as follows: In Section 2 we propose a construction method of quantum stabilizer codes from algebraic curves and discuss decoding process of the constructed codes. In Section 3.1 we construct an asymptotically good sequence of quantum codes as an example of the proposed construction method. In Section 3.2 we improved the construction of asymptotically good sequence in [2] as a byproduct of the construction in Section 3.1, and compare the sequences in Section 3 with the known asymptotically good sequences [2, 8] in Figure 1.

2 Quantum stabilizer codes from algebraic curves

2.1 Construction

We shall use the formalism of algebraic function fields instead of algebraic curves. Notations used are exactly the same as those in Stichtenoth's textbook [21].

Proposition 2 *Let $F/\mathbf{F}_q$ be an algebraic function field of one variable, σ an automorphism of order 2 of F not moving elements in $\mathbf{F}_q$, and $P_1, \ldots, P_n$ pairwise distinct places of degree one such that $\sigma P_i \neq P_j$ for all i, $j = 1, \ldots, n$. Let us introduce a condition on a differential η:*

$$\begin{cases} v_{P_i}(\eta) = v_{\sigma P_i}(\eta) = -1, \\ \mathrm{res}_{P_i}(\eta) = 1, \\ \mathrm{res}_{\sigma P_i}(\eta) = -1. \end{cases} \tag{3}$$

The existence of such η is guaranteed by the strong approximation theorem of discrete valuations [21, Theorem I.6.4]. Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$. Define

$$C(G) = \{(f(P_1), \ldots, f(P_n), f(\sigma P_1), \ldots, f(\sigma P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbf{F}_q^{2n}.$$

Let

$$H = (P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n) - G + (\eta),$$

where η is as Eq. (3). Then we have $C(G)^{\perp \mathrm{s}} = C(H)$.

Proof. In the following argument, $\vec{x} = (x_1, \ldots, x_{2n})$ and $\vec{y} = (y_1, \ldots, y_{2n})$. By Proposition VII.3.3 in [21] and the assumption on σ and G, we have

$$\begin{aligned} & (x_1, \ldots, x_{2n}) \in C(G) \\ \iff & (x_{n+1}, \ldots, x_{2n}, x_1, \ldots, x_n) \in C(G). \end{aligned} \tag{4}$$

The assertion is proved as follows:

$$\begin{aligned} & \vec{x} \in C(H) \\ \iff & \forall \vec{y} \in C(G),\ \sum_{i=1}^{n} x_i y_i - \sum_{i=n+1}^{2n} x_i y_i = 0 \text{ (by Corollary 2.7 of [20])} \\ \iff & \forall \vec{y} \in C(G),\ \sum_{i=1}^{n} x_i y_{n+i} - \sum_{i=1}^{n} x_{n+i} y_i = 0 \text{ (by Eq. (4))} \\ \iff & \vec{x} \in C(G)^{\perp \mathrm{s}}. \end{aligned}$$

■

Corollary 3 *Notations as in Proposition 2. Assume further that $G \geq H$. Then we can construct an $[[n, k, d]]$ quantum code Q, where*

$$k = \dim G - \dim(G - P_1 - \cdots - P_n - \sigma P_1 - \cdots - \sigma P_n) - n. \tag{5}$$

For the minimum distance d of Q, we have

$$d \geq n - \left\lfloor \frac{\deg G}{2} \right\rfloor. \tag{6}$$

Proof. Theorem 1 and Proposition 2 show that we can construct a quantum code from $C(G)$ because $C(G) \supseteq C(G)^{\perp \mathrm{s}} = C(H)$. By Theorem 1 we have $k = \dim C(G) - n$. Theorem II.2.2 of [21] asserts

$$\dim C(G) = \dim G - \dim(G - P_1 - \cdots - P_n - \sigma P_1 - \cdots - \sigma P_n),$$

which shows Eq. (5).

We shall prove Eq. (6). Suppose that $w(f(P_1), \ldots, f(\sigma P_n)) = \delta \neq 0$ for $f \in \mathcal{L}(G)$. Then there exists a set $\{i_1, \ldots, i_{n-\delta}\}$ such that $f(P_{i_1}) = f(\sigma P_{i_1}) = \cdots = f(P_{i_{n-\delta}}) = f(\sigma P_{i_{n-\delta}}) = 0$, which implies $f \in \mathcal{L}(G - \sum_{j=1}^{n-\delta}(P_{i_j} + \sigma P_{i_j}))$. Since $f \neq 0$, we have

$$\begin{aligned}
& \dim\left(G - \sum_{j=1}^{n-\delta}(P_{i_j} + \sigma P_{i_j})\right) > 0 \\
\Longrightarrow\ & \deg\left(G - \sum_{j=1}^{n-\delta}(P_{i_j} + \sigma P_{i_j})\right) \geq 0 \\
\Longleftrightarrow\ & \deg G - 2(n - \delta) \geq 0 \\
\Longleftrightarrow\ & 2\delta \geq 2n - \deg G \\
\Longleftrightarrow\ & \delta \geq n - \left\lfloor \frac{\deg G}{2} \right\rfloor.
\end{aligned}$$

■

The above construction provides good codes only when q is large as the classical algebraic geometry codes. For small q, we construct a q-ary quantum code from a q^m-ary one by

Theorem 4 (Ashikhmin and Knill [1]) *Let m be a positive integer, $\{\alpha_1, \ldots, \alpha_m\}$ an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^m}$. Define $\mathbf{F}_q$-linear maps $\alpha : \mathbf{F}_q^m \to \mathbf{F}_{q^m}$ sending $(x_1, \ldots, x_m)$ to $x_1\alpha_1 + \cdots + x_m\alpha_m$, and $\beta : \mathbf{F}_q^m \to \mathbf{F}_{q^m}$ sending $(x_1, \ldots, x_m)$ to*

$$(\alpha_1, \ldots, \alpha_m) M \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \mathbf{F}_{q^m},$$

where M is an $m \times m$ matrix defined by $M_{ij} = \mathrm{Tr}_q^{q^m}(\alpha_i\alpha_j)$ with the trace function $\mathrm{Tr}_q^{q^m}$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$. For $C \subseteq \mathbf{F}_{q^m}^n$, let $\gamma(C) = \{(\alpha^{-1}(x_1), \ldots, \alpha^{-1}(x_n), \beta^{-1}(x_{n+1}), \ldots, \beta^{-1}(x_{2n})) \mid (x_1, \ldots, x_{2n}) \in C\} \subseteq \mathbf{F}_q^{2mn}$. If $C^{\perp\mathrm{s}} \subseteq C$ for $C \subseteq \mathbf{F}_{q^m}^{2n}$, then $(\gamma(C))^{\perp\mathrm{s}} \subseteq \gamma(C)$. We also have $d(\gamma(C) \setminus (\gamma(C))^{\perp\mathrm{s}}) \geq d(C \setminus C^{\perp\mathrm{s}})$.

2.2 Determination of the error operator from measurement outcomes

The decoding process of a quantum stabilizer code is usually proceeded as follows [6]: One measures each observable corresponding to a generator of the stabilizer group of the code, then determines which unitary operator on $\mathcal{H}^{\otimes n}$ should be applied to the received state.

In the determination of the operator from measurement outcomes we have to solve the following problem.

Problem 5 *Let C be an $(n+k)$-dimensional subspace of $\mathbf{F}_q^{2n}$ such that $C^{\perp\mathrm{s}} \subseteq C$. Given $s_1, \ldots, s_{n-k} \in \mathbf{F}_q$, find a vector $\vec{e}$ having the minimum weight (2) in the set $\{\vec{y} \in \mathbf{F}_q^{2n} \mid \langle \vec{y}, \vec{b}_i \rangle_{\mathrm{s}} = s_i$ for $i = 1, \ldots, n-k\}$, where $\{\vec{b}_1, \ldots, \vec{b}_{n-k}\}$ is a basis of $C^{\perp\mathrm{s}}$.*

If there exists a vector $\vec{e} \in \mathbf{F}_q^{2n}$ such that $\langle \vec{e}, \vec{b}_i \rangle_{\mathrm{s}} = s_i$ for $i = 1, \ldots, n-k$ and that

$$2w(\vec{e}) + 1 \leq n - \left\lfloor \frac{\deg G}{2} \right\rfloor, \tag{7}$$

where $\{\vec{b}_1, \ldots, \vec{b}_{n-k}\}$ is a basis of $C(G)^{\perp\mathrm{s}} = C(H)$ constructed in Corollary 3, then we can efficiently find $\vec{e}$ from $s_1, \ldots, s_{n-k}$ as follows.

The algorithm of Farrán [9] efficiently finds the unique vector $\vec{x}$ having the minimum *Hamming* weight $w_{\mathrm{H}}(\vec{x})$ in the set $\{\vec{y} \in \mathbf{F}_q^{2n} \mid \langle \vec{y}, \vec{b}_i \rangle = s_i$ for $i = 1,$

$\ldots, n-k\}$ from given $s_1, \ldots, s_{n-k}$, provided that $2w_{\mathrm{H}}(\vec{x})+1 \leq 2n - \deg G$, where $\langle \vec{x}, \vec{b}_i \rangle$ is the standard inner product of $\vec{x}$ and $\vec{b}_i$ and $\{\vec{b}_1, \ldots, \vec{b}_{n-k}\}$ is a basis of $C(H)$.

Let $\vec{e} = (e_1, \ldots, e_{2n})$ and $\vec{e'} = (-e_{n+1}, \ldots, -e_{2n}, e_1, \ldots, e_n)$. Then $s_i = \langle \vec{e'}, \vec{b}_i \rangle = \langle \vec{e}, \vec{b}_i \rangle_{\mathrm{s}}$. Since $w_{\mathrm{H}}(\vec{e'}) \leq 2w(\vec{e})$, Eq. (7) implies

$$2w_{\mathrm{H}}(\vec{e'}) + 1 \leq 2n - \deg G,$$

and the algorithm of Farrán finds $\vec{e'}$ from $s_1, \ldots, s_{n-k}$ correctly. We can easily find $\vec{e}$ from $\vec{e'}$.

3 Asymptotically good sequence of quantum codes

3.1 Sequence of codes by the proposed method

In this section we construct an asymptotically good sequence of binary quantum codes from the Garcia-Stichtenoth function field [10]. Let $F_i = \mathbf{F}_{q^2}(x_1, z_2, \ldots, z_i)$ with

$$\begin{aligned} z_i^q + z_i - x_{i-1}^{q+1} &= 0, \\ x_i &= z_i / x_{i-1}. \end{aligned}$$

Proposition 6 *For an integer $m \geq 2$ there exists a sequence of $[[n_i, k_i, d_i]]$ binary quantum stabilizer codes such that*

$$\begin{aligned} \lim_{i\to\infty} n_i &= \infty, \\ \liminf_{i\to\infty} k_i/n_i &\geq R_m^{(1)}(\delta), \\ \liminf_{i\to\infty} d_i/n_i &\geq \delta, \end{aligned}$$

where

$$R_m^{(1)}(\delta) = 1 - \frac{2}{2^m - 1} - 4m\delta.$$

Proof. We shall consider the Garcia-Stichtenoth function field F_i over $\mathbf{F}_{2^{2m}}$ with $i \geq 2$. Let $q = 2^m$. Since the Galois group of F_i/F_{i-1} is isomorphic to the additive group of $\mathbf{F}_2^m$ [10, Proposition 1.1 (i)], there exists an automorphism $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$ of order 2.

Let $n_i = (q^2-1)q^{i-1}/2$, and $y = x_1^{q^2-1} - 1$. The zero divisors of y consist of $2n_i$ places of degree one [10, Section 3]. Let F_i^σ be the fixed field of σ. Let Q be a zero of y. There exists a zero Q' of y such that $Q' \neq Q$ and $Q \cap F_i^\sigma = Q' \cap F_i^\sigma$. Since F_i/F_i^σ is Galois, by Theorem III.7.1 of [21] we have $\sigma Q = Q'$. Therefore we can write the zero divisor of y as $P_1 + \sigma P_1 + \cdots + P_{n_i} + \sigma P_{n_i}$ such that $\sigma P_j \neq P_l$ for all j, l. Let $\eta = dy/y = x_1^{q^2-2} dx_1/y$. By Proposition VII.1.2 of [21], η satisfies the condition (3).

Let $G_0' = (\eta) + P_1 + \sigma P_1 + \cdots + P_{n_i} + \sigma P_{n_i}$, and P_∞ the unique pole of x_1 in F_i. We have

$$G_0' = (q^2-2)(x_1) - (q^2-1)v_{P_\infty}(x_1)P_\infty + (dx_1).$$

The different exponent of F_i/F_1 is even at every place of F_i (see the text below Lemma 2.9 of [10]). Hence the discrete valuation of (dx_1) is even at every place of F_i by Remark IV.3.7 of [21]. Observe that $v_{P_\infty}(x_1) = -q^{i-1}$ [10]. Therefore the valuation of the divisor G_0' is an even integer at every place of F_i. Define $G_0 = G_0'/2$. We have

$$\begin{aligned} \deg G_0 &= \frac{2n_i + \deg(dx_1)}{2} \\ &= \frac{2n_i + 2g_i - 2}{2} \\ &= n_i + g_i - 1, \end{aligned}$$

where g_i is the genus of $F_i/\mathbf{F}_{q^2}$.

Let j be a nonnegative integer. Since $\sigma(G_0 + jP_\infty) = G_0 + jP_\infty$, it satisfies the condition on G in Proposition 2. Let $H = (P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n) - (G_0 + jP_\infty) + (\eta) = G_0 - jP_\infty$. Since $G + jP_\infty \geq H$, $C(G + jP_\infty)^{\perp \mathrm{s}} \subseteq C(G + jP_\infty)$. By Corollary 3 we can construct an $[[n_i, k_{ij}, d_{ij}]]$ quantum stabilizer code with

$$k_{ij} \geq j,\ d_{ij} \geq (n_i - g_i - j + 1)/2.$$

Let R be a real number such that $0 \leq R \leq 1$, and set j to $\lfloor R n_i \rfloor$. By Theorem 4 we can construct a sequence of $[[n_i, k_i, d_i]]$ binary quantum stabilizer codes with

$$\begin{aligned} \liminf_{i\to\infty} k_i/n_i &\geq R, \\ \liminf_{i\to\infty} d_i/n_i &\geq \delta = \frac{1 - R - 2/(2^m-1)}{4m}, \end{aligned}$$

because n_i/g_i converges[1] to $(2^m - 1)/2$ as $i \to \infty$ [10]. Simple calculation shows $R = R_m^{(1)}(\delta)$. ■

By choosing an appropriate value m for every δ, we can construct a sequence of $[[n_i, k_i, d_i]]$ binary quantum codes with

$$\liminf_{i\to\infty} k_i/n_i \geq R^{(1)}(\delta),\ \liminf_{i\to\infty} d_i/n_i \geq \delta,$$

where

$$R^{(1)}(\delta) = R_m^{(1)}(\delta) \text{ for } \frac{2^{m-1}}{(2^m-1)(2^{m+1}-1)} \leq \delta \leq \frac{2^{m-2}}{(2^{m-1}-1)(2^m-1)}.$$

The function $R^{(1)}(\delta)$ is plotted in Figure 1.

3.2 Improvement of the Ashikhmin-Litsyn-Tsfasman construction

In [2] Ashikhmin et al. constructed an asymptotically good sequence of binary quantum codes from self-orthogonal classical algebraic geometry codes. In their construction they do not use at least g points on the curve (see Remark below Theorem 4 of [2]), where g is the genus of the curve.

By [21, Proposition VII.1.2] we have $C(G_0+jP_\infty) \supseteq C(G_0+jP_\infty)^\perp$ for the code $C(G_0+jP_\infty)$ over $\mathbf{F}_{2^{2m}}$ constructed in the proof of Proposition 6, where $C(G_0+jP_\infty)^\perp$ is the dual code of $C(G_0+jP_\infty)$ with respect to the standard inner product. In the construction of $C(G_0+jP_\infty)$ we asymptotically use all the points on the curve. Therefore we can construct a better sequence of binary quantum codes if we use $C(G_0+jP_\infty)$ in the construction of Ashikhmin et al.

Let us calculate the asymptotic parameters of the sequence constructed by the method of Ashikhmin et al. with $C(G_0+jP_\infty)$. Let N_i $(= 2n_i)$ be the code length of $C(G_0+jP_\infty)$ as a classical linear code. We have

$$\dim C(G_0+jP_\infty) \geq \dim(G_0+jP_\infty) \geq j + N_i/2,$$

and the minimum Hamming distance of $C(G_0+jP_\infty)$ is not less than

$$N_i/2 - g_i + 1 - j.$$

[1] In the versions 1 and 2 of this eprint, the author miscalculated $\lim_{i\to\infty} n_i/g_i$ as $2^m - 1$, which led the wrong value of $R_m^{(1)}(\delta)$. The author apologize for misleading the reader.

By the construction of binary quantum codes in [2], from the inclusion of classical codes

$$\begin{aligned} & C\left(G_0 + \left(\left(\frac{1}{2} - \delta'\right) N_i - g_i + 1\right) P_\infty\right)^\perp \\ \subset\ & C\left(G_0 + \left(\left(\frac{1}{2} - \delta'\right) N_i - g_i + 1\right) P_\infty\right) \\ \subset\ & C\left(G_0 + \left(\left\lfloor\left(\frac{1}{2} - \frac{2}{3}\delta'\right) N_i\right\rfloor - g_i + 1\right) P_\infty\right) \end{aligned}$$

for $0 \le \delta' \le 1/2 - g_i/N_i$, we can construct $[[N_i, k_i, d_i]]$ binary quantum codes with

$$k_i \ge \left(1 - \frac{5}{3}\delta'\right) N_i - 2g_i + 1,\ d_i \ge \frac{\delta' N_i}{2m}.$$

Since $\lim_{i\to\infty} N_i/g_i = 2^m - 1$ [10], by setting $\delta = \delta'/2m$ we have

$$\liminf_{i\to\infty} \frac{k_i}{N_i} \ge R_m^{(\mathrm{ALT})}(\delta),\ \liminf_{i\to\infty} \frac{d_i}{N_i} \ge \delta,$$

where

$$R_m^{(\mathrm{ALT})}(\delta) = 1 - \frac{10}{3}m\delta - \frac{2}{2^m - 1}. \tag{8}$$

It is clear that Eq. (8) is larger than Eq. (21) of [2].

By choosing an appropriate value m for every δ, we can construct a sequence of $[[N_i, k_i, d_i]]$ binary quantum codes with

$$\liminf_{i\to\infty} \frac{k_i}{N_i} \ge R^{(\mathrm{ALT})}(\delta),\ \liminf_{i\to\infty} \frac{d_i}{N_i} \ge \delta,$$

where $R^{(\mathrm{ALT})}(\delta) = R_m^{(\mathrm{ALT})}(\delta)$ for

$$\frac{3 \cdot 2^m}{5(2^m - 1)(2^{m+1} - 1)} \le \delta \le \min\left\{\frac{5}{84}, \frac{3 \cdot 2^{m-1}}{5(2^{m-1} - 1)(2^m - 1)}\right\}.$$

Ashikhmin et al. [2] constructed an asymptotically good sequence of binary quantum codes from algebraic curves. Chen et al. [8] constructed a sequence based on the idea in [22] better than [2] in certain range of parameters. Their sequences and the sequences in this section are compared in Figure 1. Note that Chen [7] also proposed the same construction of quantum codes as [2].

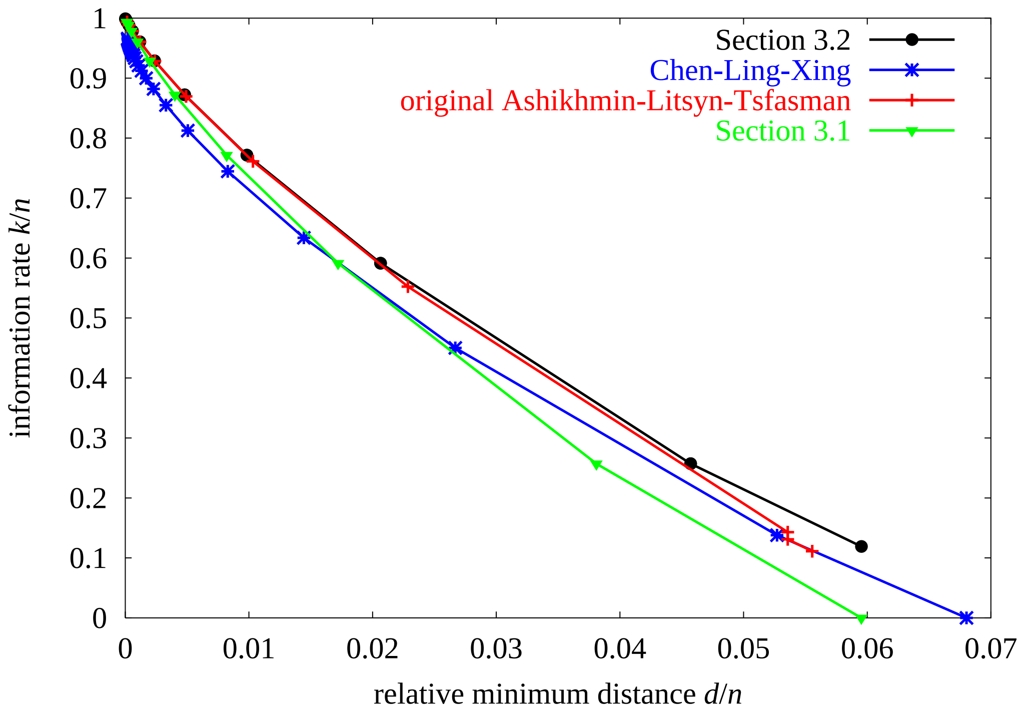

Figure 1: Asymptotically good sequences of quantum codes (color)

References

[1] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. May 2000, quant-ph/0005008.

[2] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman. Asymptotically good quantum codes. *Phys. Rev. A*, 63(3):032311, Mar. 2001, quant-ph/0006061.

[3] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. June 2001, quant-ph/0106052.

[4] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, Nov. 1992.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, Jan. 1997, quant-ph/9605005.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quan-

tum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, July 1998, quant-ph/9608006.

[7] H. Chen. Some good quantum error-correcting codes from algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 47(5):2059–2061, July 2001, quant-ph/0107102.

[8] H. Chen, S. Ling, and C. Xing. Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound. *IEEE Trans. Inform. Theory*, 47(5):2055–2058, July 2001.

[9] J. I. Farrán. Decoding algebraic geometry codes by a key equation. *Finite Fields Appl.*, 6(3):207–217, July 2000, math.AG/9910151.

[10] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields, attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121(1):211–222, July 1995.

[11] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54(3):1862–1868, Sept. 1996, quant-ph/9604038.

[12] S. Kak. The initialization problem in quantum computing. *Found. Phys.*, 29(2):267–279, Feb. 1999, quant-ph/9811005.

[13] E. Knill. Non-binary unitary error bases and quantum codes. Aug. 1996, quant-ph/9608048.

[14] R. Matsumoto. Fidelity of a t-error correcting quantum code with more than t errors. *Phys. Rev. A*, 64(2):022314, Aug. 2001, quant-ph/0011047.

[15] W. W. Peterson and E. J. Weldon, Jr. *Error-Correcting Codes.* MIT Press, Cambridge, Massachusetts, 2nd edition, 1972.

[16] J. Preskill. Lecture Notes for Physics 229: Quantum Information and Computation, `http://www.theory.caltech.edu/people/preskill/ph229`, 1998.

[17] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, Sept. 1999, quant-ph/9703048.

[18] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):2493–2496, Oct. 1995.

[19] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, July 1996.

[20] H. Stichtenoth. Self-dual Goppa codes. *J. Pure Appl. Algebra*, 55(1,2):199–211, Nov. 1988.

[21] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin, 1993.

[22] C. Xing, H. Niederreiter, and K. Y. Lam. A generalization of algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(7):2498–2501, Nov. 1999.